

REMARKS

Claims 1-67 are pending. Claims 1-67 stand rejected under 35 U.S.C § 103(a) as being unpatentable over U.S. Patent No. 5,457,747 to Drexler et al. in view of Mark Rechlin (Fingerprint Technology Makes for Best ID System).

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-67 remain in the case for consideration.

The Applicant requests that the Examiner treat the Office Action as non-final, as the new grounds for rejection were not necessitated by the Applicant's amendment. The previous amendment made no substantive changes to the claims. It made only three types of changes: it removed some language that might have been considered indefinite; it corrected antecedent basis problems with claims 1 and 32, and it corrected typographical errors in claims 7, 32, and 36-37. In short, the scope of the claims has been neither narrowed nor enlarged by the amendments, and therefore did not necessitate the new grounds for rejection. Accordingly, by relying on a new reference, previously uncited, the Examiner has raised new grounds for rejection that were not necessitated by an amendment, and the Office Action should not be considered final.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Referring to claim 1, the invention is directed toward a method for tokenless biometric authorization. At least one communication is formed. A user electronically submits a registration biometric sample. The registration biometric sample is electronically transmitted via a public communications network. The registration biometric sample is then stored in a master electronic identifier. The user then submits a bid biometric sample, which is transmitted to an electronic identifier. The user is identified by comparing the bid biometric sample with a registration biometric sample. Upon successful identification, an electronic communication is authorized. The entire method can be carried out without using smartcards or magnetic stripe cards.

Referring to claim 32, the invention is directed toward a system for tokenless biometric authorization. The system includes a communication input apparatus, which includes a data entry device to form an electronic communication. A biometric input apparatus includes a device to scan a biometric sample from the user. A master electronic identifier includes a database to store biometric samples from registered users and a comparator to compare received biometric samples with previously stored biometric samples. The system also includes a public network to transmit data between the biometric input

apparatus and the master electronic identifier and an electronic communication authorization to authorize execution of a communication upon successful identification of the user. The system can operate without using smartcards or magnetic stripe cards.

In contrast, Drexler teaches a system for deterring fraudulent use of cards. The user has a card, which stores both the user's biometric sample and limits on the use of the card to obtain benefits. The user initially records his biometric sample on the card. Then, when the user presents the card to obtain services, the user provides another biometric sample, which is compared with the biometric data stored on the card. If the biometric sample matches the biometric data stored on the card, then the user limit data is accessed from the card, and if the use requested by the person is authorized, the user receives the desired benefits.

The Examiner acknowledges that Drexler fails to teach authorizing an electronic communication without using a smartcard or magnetic stripe card. The Examiner cites the Rechtin newspaper article as teaching this concept. The Examiner then concludes that it would be obvious to modify Drexler to take advantage of Rechtin.

It is not possible to adapt Drexler to take advantage of the teaching of Rechtin. There are several reasons why this is so. First, as noted in the Response to the Office Action dated April 9, 2003, Drexler relies on the use of a card to store the biometric sample. Thus, Drexler teaches away from the invention. A person of ordinary skill in the art would not think to combine Drexler, which teaches a system requiring a card, with Rechtin, which suggests using biometrics without a card.

Second, Rechtin predates Drexler. Consequently, Drexler, at the time of his invention, had as part of the public knowledge the information described in Rechtin. But Drexler chose instead to design a system that uses a card, even though he knew it had been suggested designing biometric systems that did not use a card. This suggests that Drexler himself, probably the person best qualified to indicate how his invention could be adapted, did not believe his invention could be modified to operate without a card. Significantly, Rechtin does not provide an enabling description of any method or system employing the fingerprint comparison machines mentioned in the article.

Third, Rechtin quoted the research and development director of one company stating that adoption of cardless biometric systems would be ubiquitous within 5-10 years of the publication date of Rechtin. As Rechtin was published in 1990, Rechtin expected cardless biometric systems to be "ubiquitous" by 2000. Yet here we are in 2004, still relying on non-biometric access control systems. Clearly, Rechtin and the supposed experts he quoted underestimated the complexity of biometric systems. This suggests that the modification of

Drexler according to Rechten is not as simple as the Examiner believes, and therefore not an obvious combination.

Fourth, even if it were possible to modify Drexler according to the teaching of Rechten (a position the Applicant disputes), the claimed combination would not be obvious. As Drexler teaches a system that relies on a card, adapting Drexler to eliminate the card would require completely redesigning the system. For example, Drexler uses the card to identify the user, and then uses the biometric stored on the card to verify the user's identity. To eliminate the card as suggested by the Examiner would require introducing into Drexler some other way to identify the user, so that the biometrics can continue to be used to verify the user's identity.

The Examiner may be thinking that Drexler could be modified to use the biometric to identify the user, as claimed. But such a modification would eliminate the need for Drexler. The Applicant points out that the purpose of Drexler, *as stated in the title of Drexler*, is to provide a system to *verify* a user that avoids fraud. If biometrics were used to *identify* the user, there would be no concern about fraud. (Indeed, the claimed invention addresses specifically this issue.) Without a concern about fraud, Drexler becomes irrelevant. Thus, Drexler cannot be modified from a system that uses biometrics to *verify a user's identity* to one that *identifies a user*.

In addition, there are other deficiencies of Drexler, raised in the Response to the Office Action dated April 9, 2003, that the Examiner has failed to address. First, the invention stores the registration biometric samples in a master electronic identifier, which includes a database of registration biometric samples from many users. Unless many people share the card of Drexler (a totally impractical idea), it will only store the biometric data for one person. Therefore, the Drexler card cannot be a database storing registration biometric samples from many users.

Second, as the Drexler card stores only one user's biometric data, Drexler cannot perform user *identification*. Identification is the process of determining a user's identity. In effect, identification answers the question "Who am I?" Identification assumes that there is no information already suggesting the user's identity. In contrast, *verification* answers the question "Am I who I say I am?" Because there is only one user's biometric data stored on the Drexler card, the user has already identified himself, and is asking the system to *verify his identity*.

Another way to look at the difference between identification and verification is to consider what happens in the equipment performing the processes. In identification, the

offered biometric sample is compared with at least a subset of the registered biometric samples, so that the system can say, "Of all the registered biometric samples I looked at, the offered biometric sample most likely matches this one." But in verification, the offered biometric sample is compared with *only one* registered biometric sample: the one associated with the person the user claims to be. The system says either "He is whom he says he is," or "He is not whom he says he is." The system makes no effort to compare the offered biometric sample with any other registered biometric sample to determine the user's true identity.

To give yet another explanation of the difference between identification and verification, consider the situation where a person is attempting to commit fraud and assert that he is someone else. (Note that avoiding fraud is the stated purpose of Drexler, both in the title and technical field of Drexler.) Drexler would compare the offered biometric sample of the criminal with that of the card, and determine that they do not match. Drexler would then deny the criminal the benefits he sought. In contrast, the invention would identify the criminal (assuming the criminal has registered with the system). This means that the police could be sent to arrest the criminal knowing his identity. Drexler cannot accomplish this, because Drexler does not perform identification.

Drexler mentions a library, which stores biometric information. But, as described at column 8, lines 7-27, Drexler uses the library only to re-verify the user's identity as an anti-fraud measure, and not for identification.

Third, Drexler does not teach transmission, either of the registration biometric sample or of the bid biometric sample. In Drexler, the registration biometric sample is stored on the card, which is in the user's possession at the time of registration. And both the registered biometric sample and the offered biometric sample are locally available in Drexler when the user requests benefits. Drexler can compare the offered biometric sample with the biometric data stored on the card at the machine at the time the user makes the request for benefits: no transmission anywhere is needed. In contrast, in the invention the registration biometric sample is stored in the master electronic indicicator. The master electronic indicicator is typically remote (and secure) relative to the user's location, and therefore the registration biometric sample is transmitted from the place where it is received to the master electronic indicicator. Similarly, the place where the user offers the bid biometric sample is typically remote from where the system performs identification of the user, and so the bid biometric sample is transmitted to the electronic indicicator.


Because neither Drexler nor Rehtin teach some of the features of the invention, because there is no motivation to combine Drexler and Rehtin, and because Drexler cannot be modified according to Rehtin (even if there were an enabling description in Rehtin and a motivation to combine the references), claims 1 and 32 are patentable under 35 U.S.C. § 103(a) over Drexler in view of Rehtin. Accordingly, claims 1-67 are allowable.

Referring to claims 2-31 and 33-67, the Examiner did not present a prima facie argument that the inventions are obvious over Drexler in view of Rehtin. The Examiner simply stated that these claims disclose the same inventive concepts as in claims 1 and 32. While claims 2-31 and 33-67 further define the inventions of claims 1 and 32, respectively, they also add further limitations that distinguish claims 2-31 and 33-67 over claims 1 and 32, and therefore are not the same inventive concepts. As the Examiner did not indicate where the limitations of claims 2-31 and 33-67 are specifically taught within Drexler or Rehtin, claims 2-31 and 33-67 should therefore be allowable with claims 1 and 32. Moreover, these claims add further inventive features that are patentable in their own right over Drexler in view of Rehtin: e.g., the rule-module of claims 17 and 49, and the use of a personal identification code in claims 66-67.

For the foregoing reasons, reconsideration and allowance of claims 1-67 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.



Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM
1030 SW Morrison Street
Portland, OR 97205
(503) 222-3613
Customer No. 20575

Page 22 of 22

I hereby certify that this correspondence is being transmitted to the U.S. Patent and Trademark Office via facsimile number (703) 872-9306, on January 26, 2004.

Signature



Ariel S. Rogson